



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/666,377	09/20/2000	Alexander G. Dickinson	48556.00005	6149

23767 7590 06/28/2004

PRESTON GATES ELLIS & ROUVELAS MEEDS LLP  
1735 NEW YORK AVENUE, NW, SUITE 500  
WASHINGTON, DC 20006

EXAMINER

ZIA, MOSSADEQ

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 06/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/666,377

Applicant(s)

DICKINSON ET AL. *dn*

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09/20/2000.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-42 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |                                                                                                                                         |                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                                             | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                                    | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>14</u> . | 6) <input type="checkbox"/> Other: _____                                                |

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

1. Claim 12-42 is rejected under 35 U.S.C. 102(e) as being anticipated by Patent No. 6,691,232 Wood et al.
2. Regarding claim 12, Wood shows a system for graded authentication comprising user data obtained from a user during at least one previously successful authentication attempt, circumstantial data associated with the at least one previously successful authentication attempt, and a trust engine which generates a level of trust associated with a current authentication attempt based on the comparison of circumstantial data associated with the current authentication attempt with the circumstantial data associated with the at least one previously successful authentication attempt (Wood, col. 6, line 10-15).
3. Regarding claim 13, Wood shows claim 12 above, and further show the user data represents intent to assent to a transaction (order processing system for ecommerce, Wood, col. 5, line 39).
4. Regarding claim 14, Wood shows claim 12 above, and further show the circumstantial data represents a network address associated with the authentication attempt (source of request, Wood, col. 6, line 32-33).

Art Unit: 2134

5. Regarding claim 15, Wood shows claim 12 above, and further show the circumstantial data represents a time stamp associated with the authentication attempt (time of request, Wood, col. 6, line 31-32).

6. Regarding claim 16, Wood shows claim 12 above, and further show the level of trust is also based upon the comparison of the user data to previously stored user data (session token... associate prior authentication of login credentials, Wood, col. 8, line 41-44).

7. Regarding 17, Wood shows a method for authenticating a user comprising:

obtaining user data associated with an authentication operation (password, Wood, col. 2, line 35, 42);

obtaining metadata (session token) related to the authentication operation (Wood, col. 8, line 30-36);

comparing the metadata with previously stored data (session continuity, Wood, col. 8, line 42-43);

determining a level of trust associated with the authentication operation (Wood, col. 8, line 36-37).

8. Regarding claim 18, Wood shows claim 17 above, and further show the user data associated with the authentication operation represents the intent of a user to assent to a transaction (Wood, col.5, line 51-55).

9. Regarding claim 19, Wood shows claim 18 above, and further show the metadata related to the authentication operation are made available at a later time to contest a repudiation of the authentication operation by the user (Wood, col. 8, line 41-44).

10. Regarding claim 20, Wood shows claim 17 above, and further show the act of determining a level of trust associated with the authentication operation comprises assigning a percentage to the authentication operation which represents the degree of confidence in the authentication of the user (authenticated to a particular trust level, Wood, col. 6, line 4-10).

11. Regarding claim 21, Wood shows claim 17 above, and further show the determining an intermediate level of trust associated with the metadata based upon the comparison of the metadata with the previously stored data (session token... associate prior authentication of login credentials, Wood, col. 8, line 41-44).

12. Regarding claim 22, Wood shows claim 21 above, and further show the act of determining an intermediate level of trust comprises assigning a percentage to the metadata which represents the degree of correspondence between the metadata and the previously stored data (Wood, col. 8, line 30-32).

13. Regarding claim 23, Wood shows claim 22 above, and further show the act of determining a level of trust associated with the authentication operation comprises multiplying the percentage representing the intermediate level of trust and a percentage which represents a degree of correspondence between the user data (trust level information, Wood, col. 8, line 36-37) and the previously stored data (Wood, col. 7, line 1-7).

14. Regarding claim 24, Wood shows claim 23 above, and further show additional factors are used to weight the percentage representing the intermediate level of trust and the percentage which represents the degree of correspondence between the user data and the previously stored data differently (trust level mapping, col. 14, line 42-43, 49-51).

15. Regarding claim 25, Wood shows a method for authenticating a user comprising:

Art Unit: 2134

obtaining user data associated with a authentication operation (password, Wood, col. 2, line 35, 42);

obtaining metadata (credentials) related to the authentication operation (biometric techniques, Wood, col. 5, line 57-58, 63); and

determining a level of trust associated with the authentication operation based on metadata (Wood, col. 2, line 42-43).

16. Regarding claim 26, Wood shows claim 25 above, and further show the act determining a level of trust compares the metadata with previously stored data (Wood, col. 8, line 36-37).

17. Regarding claim 27, Wood shows claim 25 above, and further show providing the user with a plurality of authentication techniques, which may be used to generate the user data (biometric techniques, Wood, col. 5, line 60-64).

18. Regarding claim 28, Wood shows claim 27 above, and further show the user data is generated using more than one of the plurality of authentication techniques (login credentials, Wood, col. 18, line 40-45).

19. Regarding claim 29, Wood shows claim 28 above, and further show the user data generated using each authentication technique (Wood, col. 8, line 46-49) is compared with a different portion of a set of previously stored data (Wood, col. 8, line 41-44).

20. Regarding claim 30, Wood shows a method for grading an authentication operation that relies on a variable set of authentication techniques to obtain authentication data, the method comprising:

defining the reliability of a set of authentication techniques that may be used in an authentication operation (security policy, Wood, col. 2, line 49-55);

receiving authentication data during an authentication operation, said authentication data generated using a subset of the authentication techniques (login credentials obtained are selected from a set, Wood, col. 5, line 57-57-58);

determining the acceptability of the authentication data generated by each of the subset of authentication techniques (Wood, col. 5, line 57-64); and

defining the level of trust of the authentication operation based upon the acceptability of the authentication data and based upon the reliability of the authentication techniques used in generating the authentication data (establishing trust level, Wood, col. 3, line 8-16).

21. Regarding claim 31, Wood shows claim 30 above, and further show the act of determining the acceptability involves comparing the authentication data with previously stored enrollment data (password, certificates, Wood, col. 5, line 61-63).

22. Regarding claim 32, Wood shows claim 31 above, and further show the act of defining the reliability of a set of authentication techniques is based upon a set of circumstances associated with the previously stored enrollment data (Wood, col. 5, line 61-63, col. 8, line 36-37).

23. Regarding claim 33, Wood shows claim 30 above, and further show the act of defining the reliability of a set of authentication techniques is based upon the circumstances associated with the generation of the authentication data (Wood, col. 5, line 57-60).

24. Regarding claim 34, Wood shows an apparatus for evaluating an authentication attempt comprising:

Reliability data associated with a set of authentication techniques that may be used in an authentication attempt (Wood, col. 6, line 35-37);

a plurality of authentication instances generated using a subset of the authentication techniques (Wood, col. 3, line 50-57); and

a trust engine which determines a level of match associated with each authentication instance and assigns a level of trust for the authentication attempt based upon the level of match associated with each authentication instance and the reliability of the technique used in the each authentication instance (Wood, col. 6, line 30-34).

25. Regarding claim 35, Wood shows claim 34 above, and further show a required level of trust associated with the authentication attempt (Wood, col. 8, line 36-37).

26. Regarding claim 36, Wood shows claim 35 above, and further show the trust engine further assigns a result for the authentication based upon a comparison of level of trust associated with the authentication attempt and the required level of trust (Wood, col. 3, line 8-16, col. 8, line 36-37).

27. Regarding claim 37, Wood shows claim 35 above, and further show the required level of trust is determined by the trust engine based upon the risk associated with a successful authentication (Wood, col. 6, line 23-25).

28. Regarding claim 38, Wood shows a method for grading an authentication attempt comprising:

defining the reliability of a set of authentication techniques that may be used in an authentication attempt (security policy, Wood, col. 2, line 49-55);

receiving a plurality of authentication instances generated using a subset of the authentication techniques (login credentials obtained are selected from a set, Wood, col. 5, line 57-57-58);



determining a level of match associated with each authentication instance (Wood, col. 5, line 57-64); and

defining a level of trusted of the authentication attempt based upon level of match associated with each authentication instance and based upon the reliability of the technique used in authentication instance (establishing trust level, Wood, col. 3, line 8-16).

29. Regarding claim 39, Wood shows claim 38 above, and further show defining a required level of trust for the authentication attempt (Wood, col. 8, line 36-37).

30. Regarding claim 40, Wood shows claim 39 above, and further show assigning an authentication result to the authentication attempt based on a comparison of the level of trust for the authentication attempt and a required level of trust of the authentication attempt (Wood, col. 3, line 8-16, col. 8, line 36-37)..

31. Regarding claim 41, Wood shows claim 39 above, and further show the required level of the trust for the authentication attempt is based upon the value associated with a successful authentication (Wood, col. 6, line 35-38).

32. Regarding claim 42, Wood shows claim 39 above, and further show the required level of trust for the authentication attempt is based upon the risk associated with a successful authentication (Wood, col. 6, line 23-25).

### ***Claim Rejections - 35 USC § 103***

33. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

Art Unit: 2134

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

34. Claims 1-11, are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 6,691,232 Wood et al. in view of Patent No. 6,401,206 Khan et al.

35. Regarding claim 1, Wood show a method of performing graded authentication of a user wherein the method obtains and evaluates circumstantial data associated with an authentication attempt, the method comprising:

obtaining user data from a user during an authentication attempt (password, Wood, col. 2, line 35, 42);

obtaining circumstantial data associated with the authentication attempt (biometric techniques, Wood, col. 2, line 35, 42, col. 5, line 57-58 ); and

determining a level of trusted associated with the authentication (Wood, col. 2, line 42-43) **but fail to show** authentication attempted based on the comparison of the circumstantial data with previously stored data.

However, Khan teach the point of verification, a device is inserted into the verification machine that asks the individual to authenticate himself by carrying out a brief question (circumstantial data) and answer session (implies questions (data) where previously stored, Khan, col. 13, line 20-23).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Wood as per teaching of Khan to include the verification machine to provide an additional strong security feature (Khan, col. 13, 25-26).

Art Unit: 2134

36. Regarding claim 2, Wood and Khan shows claim 1 above, and further show act of determining the level of trust associated with the authentication attempt is further based on the comparison of the user data with previously stored data (Khan, col. 13, 24-26).

37. Regarding claim 3, Wood and Khan shows claim 1 above, and further show the previously stored data comprises in part historical record of the circumstantial data obtained during previous successful authentication for the user (session token... associate prior authentication of login credentials, Wood, col. 8, line 41-44).

38. Regarding claim 4, Wood and Khan shows claim 1 above, and further show the circumstantial data comprises an identification associated with the system from which the user data is obtained (credential associated to users, Wood, col. 4, line 49).

39. Regarding claim 5, Wood and Khan shows claim 4 above, and further show the identification comprises of a processor serial number (source number, Wood, col. 7, line 63-65).

40. Regarding claim 6, Wood and Khan shows claim 1 above, and further show the circumstantial data comprises an identification associated with the network location of the system from which the user data is obtained (source of request, Wood, col. 6, line 32-33).

41. Regarding claim 7, Wood and Khan shows claim 6 above, and further show the identification comprises an IP address (source of request, environment information, Wood, col. 2, line 56, col. 6, line 30-34).

42. Regarding claim 8, Wood and Khan shows claim 1 above, and further show the circumstantial data comprises a time associated at which the user data was obtained (time of request, Wood, col. 6, line 31-32).

Art Unit: 2134

43. Regarding claim 9, Wood and Khan shows claim 1 above, and further show the circumstantial data comprises an identifier representing the medium over which the user data is obtained (source of request, connection speed... environment information, Wood, col. 6, line 33, 36-37).

44. Regarding claim 10, Wood and Khan shows claim 1 above, and further show the circumstantial data represents more than one circumstantial aspect of the authentication attempt (in addition to password, answers to questions that are composed by the user, Abstract).

45. Regarding claim 11, Wood and Khan shows claim 10 above, and further show the circumstantial data comprises a time stamp associated with the time at which the user data was obtained (time of request, Wood, col. 6, line 31-32) and an identification associated with the network location of the system from which the user data is obtained (source of request, Wood, col. 6, line 32-33).

### *Conclusion*

46. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia  
Examiner  
Art Unit 2134

mz  
6/17/04

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100